International Journal of Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.02,Issue.17,
November-2013,
Pages:1965-1972

www.semargroups.org,
www.ijsetr.com

SMS Encryption for Mobile Communication

K. SURESH BABU[1], ALRADDADL, FAISAL SALEEMS[2]

[1]Asst Prof, Dept of CSE, School of IT, JNT University Hyderabad, A.P-India, E-mail: Kare_suresh@yahoo.co.in.
[2]Research Scholar, Dept of CNIS, School of IT, JNT University Hyderabad, A.P-India, E-mail: FFF882@gmail.com.

Abstract: Wireless peer to peer is the method by which individual users connect to each other directly, without need for a central point of management or system. It facilitate message passing between the two nodes which are directly connected. There arises a security issues for an unauthorized access to the message, hence a secured communication protocol is needed which can provide an authentication and integrity protection, which has to be establishes an end-to-end secure channel between server-side and client-side. An encryption and Decryption algorithm is used for the protocol to ensure confidentiality, integrity and non-repudiation of messages.

Keywords: Encryption and Decryption, Peer to Peer, Confidentiality, Integrity.

I. INTRODUCTION

Short Message Service(SMS) is the text communication service component of mobile communication systems, using standardized communications protocols that allow the exchange of short text messages up to 160 characters to mobile phone devices. As Short Message Service(SMS) is now widely use all over the world hence it security has become a major concern so there arise security issues for an unauthorized access to the message. A secure message system requires solving the following three problems at least.

1. Authentication: Confirm true identities between sender and receiver, and prevent impersonation attack from illegal intruders.

2. Confidentiality: Ensure that decrypted messages are accessible only to those authorized senders and receivers.

3. Integrity: Ensure that receivers can check out whether the message has been modified, and prevent tampered message.

A. Encryption and Decryption

Encryption is the process of transforming information (referred to as plaintext) using an algorithm(called cipher) to make it unreadable to anyone except those possessing special Knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). In many contexts, the word encryption also implicitly refers to the reverse process, decryption(e.g. "software for encryption" can typically also perform decryption), to make the encrypted information readable again(i.e. to make it unencrypted).

B. Peer to Peer

Peer-to-peer(P2P) or Point to point or End to End computing or networking is a distributed application architecture that partitions tasks or workloads between peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts. Peers are both suppliers and consumers of resources, in contrast to the traditional client–server model where only servers supply, and clients consumes.

II. METHODS

To overcome the security issues a blowfish algorithm is to be implemented. Reasons behind implementing blow-fish algorithm is its ability of providing high security with smaller key size which makes it very useful in resource limited device such as mobile phone, compare to others it is faster than other algorithm.

A. Analysis and Design

1. Description of the algorithm

Blowfish is a variable-length key, 64-bit block cipher. Symmetric key such as blow fish uses the same key for both encryption and decryption where as Public key algorithm use two keys, one for encryption and another for decryption. Public key used for encryption and private key used for decryption in case of public key encryption algorithms. The input is 64 bit data element A. This is divided two halves 32 bits each A1 and A2. As mentioned above this algorithm has 16 rounds and each round goes through the following steps (For I = 1 to 16).

1. A1=A1 XOR Pi
2. A2 = F(A1) XOR A2
3. Swap A1 and A2

Copyright @ 2013 SEMAR GROUPS TECHNICAL SOCIETY. All rights reserved.

After 16th round swap A1 and A2 to undo the swap. Then, A1=A1 XOR P17 and A2=A2 XOR P18. Finally, recombine A1 and A2 to get the cipher text. Function F looks like this: Divide all into four eight-bit quarters: a, b, c, and d. Then, F(A1)=((S1, a+S2, b mod 232) XOR S3,c) +S4, d mod 232. Decryption is exactly the same as encryption, except that P1, P2... P18 are used in the reverse.

B. Cipher-block chaining (CBC)

In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous cipher text block before being encrypted. This way, each cipher text block is dependent on all plaintext blocks processed up to that point. Also, to make each message unique, an initialization vector must be used in the first block.

C. Reason for selecting CBC along with Blowfish algorithm

CBC has been the most commonly used mode of operation. Its main drawbacks are that encryption is sequential(i.e., it cannot be parallelized), and that the message must be padded to a multiple of the cipher block size. Note that a one-bit change in a plaintext affects all following cipher text blocks, and a plaintext can be recovered from just two adjacent blocks of cipher text. As a consequence, decryption can be parallelized, and a one-bit change to the cipher text causes complete corruption of the corresponding block of plaintext, and inverts the corresponding bit in the following block of plaintext.

III. DESIGN

The design of the Secured Sms is divided into two parts: external and internal.

A. The external architecture

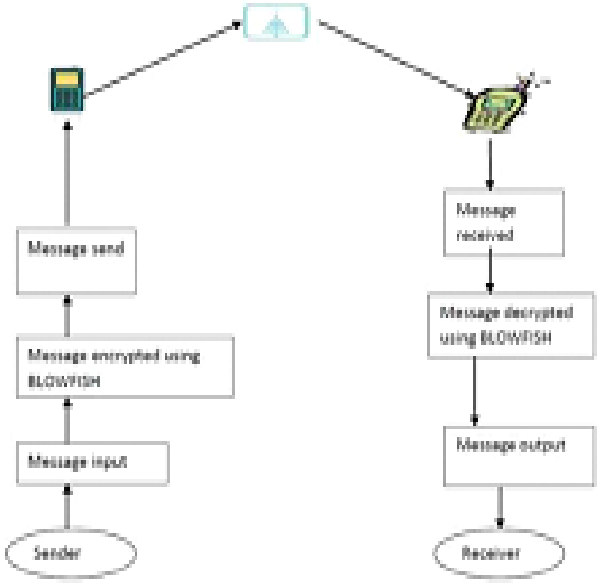

Figure 1: External structure of the system

As shown in the figure 1, the external architecture describes the overall design of the system how it works and how the components communicates with each other using the messages with respect to time.

B. The internal architecture

As shown in the figure 2, the internal architecture represents how the system internally works.

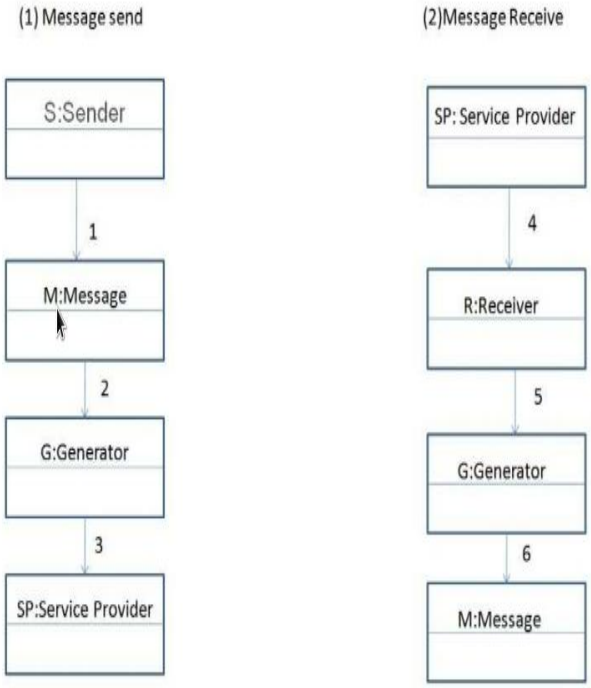

Figure 2: Internal structure of the system

C. Encrypted Sms Midlet

The Encrypted Sms MIDlet will encrypt a message using a password-based symmetric encryption algorithm and send it using a binary SMS. It is expected that the sender and the receiver have previously agreed on a common password, so there are no provisions for key exchange. The encryption algorithm used is blowfish and the digest is calculated using SHA1. Different algorithms could be used that offer higher strength. The SMS is simply a byte array containing a header, the ciphered text, and an optional message's digest. The header includes two bytes of metadata and two bytes containing the size of the cipher text. The first two bytes can be used to indicate properties of the message. The MIDlet's user interface has two screens, one for sending a

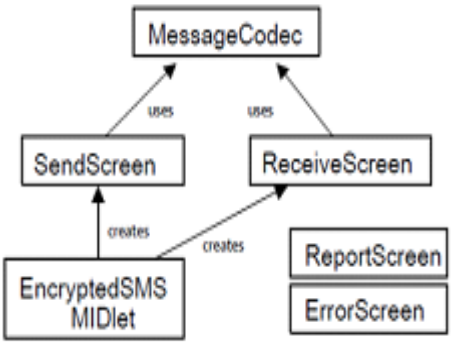

Figure 3: The process of Encrypted Sms midlet.

message and one for receiving. The sending message form contains fields for the destination number, text, password, and a choice item to indicate whether to append a digest. It also has a Send command to do the encryption and send the message. On the receiving end, the application listens for incoming messages and upon their arrival it prompts for the password to be used in the decryption process. If a message has a digest, it will also verify the integrity of the message. The figure 3 shows the encrypted SMS midlet process.

D. Short Message Service (Sms)

SMS is a communication service standardized in the GSM mobile communication systems; it can be sent and received simultaneously with GSM voice, data and fax calls. This is possible because whereas voice, data and fax calls take over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signaling path [4]. Using communications protocols such as Short Message Peer-to-Peer(SMPP) [5] allow the interchange of short text messages between mobile telephone devices as shown in Figure 4 that describe traveling of SMS between parties. SMS contains some meta-data [6]: Information about the senders(Service center number, sender number), Protocol information(Protocol identifier, Data coding scheme) and Timestamp.

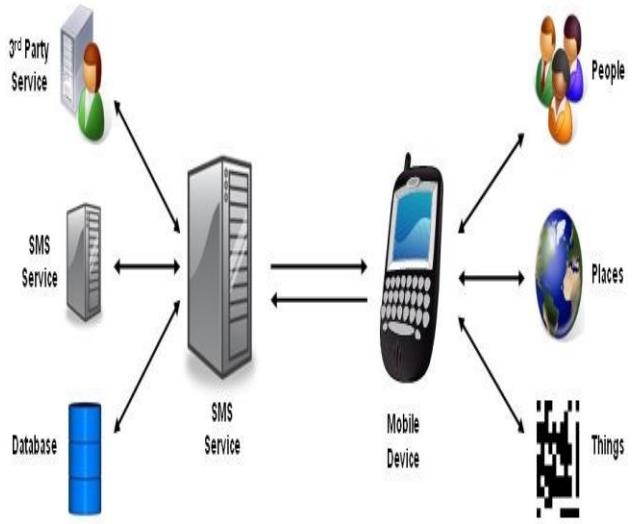

Figure 4: Travelling of SMS between mobile telephone devices

SMS messages do not require the mobile phone to be active and within range, as they will be held for a number of days until the phone is active and within range. SMS are transmitted within the same cell or to anyone with roaming capability. The SMS is a store and forward service, and is not sent directly but delivered via an SMS Center (SMSC). SMSC is a network element in the mobile telephone network, in which SMS is stored until the destination device becomes available. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the short messages [4]. SMS message packets are simple in design.

IV. SMS SECURITY

SMS travels as plain text and privacy of the SMS contents cannot be guaranteed, not only over the air, but also when such messages are stored on the handset. The contents of SMS messages are visible to the network operator's systems and personnel. The demand for active SMS based services can only be satisfied when a solution that addresses end-to-end security issues of SMS technology is available, where primary security parameters of authentication, confidentiality, integrity and non-repudiation are satisfied [9,13]. Authentication is concerned with only specific users with specific combination of device, application, memory card, and SIM card that are allowed to access corporate data. This way the users or unauthorized persons cannot change any part of the combination to obtain access to sensitive data. Confidentiality is about ensuring that only the sender and intended recipient of a message can read its content. Integrity is concerned with ensuring that the content of the messages and transactions not being altered, whether accidentally or maliciously. Non repudiation is about providing mechanisms to guarantee that a party involved in a transaction cannot falsely claim later that he/ she did not participate in that transaction[14]. An end-to-end key based encryption technology for SMS plugs the gaps in transit security of SMS. Authentication added for resident SMS security access together with encryption, addresses the confidentiality issue of SMS technology. Added features of message integrity and digital signing of SMS address integrity and Non Repudiation for SMS technology [15].

A. The Proposed Technique for Securing SMS

In this section, we describe the proposed technique used to secure SMS without increasing its length. The two main steps of this technique are the compression and encryption processes. Compression is the process of encoding SMS information using fewer bits than a un encoded representation. The purpose of this step in the proposed technique is reducing the consumption of expensive resources and reducing SMS length. SMS encryption is the art of achieving security by encoding messages to make them non-readable.

B. Sms Security Threats

Understanding the basics of SMS security opens the door to preventing some common security threats in SMS usage and implementation:

1. Message Disclosure

Since encryption is not applied to short message transmission by default, messages could be intercepted and snooped during transmission. In addition, SMS messages are stored as plain text by the SMSC before they are successfully delivered to the intended recipient. These messages could be viewed or amended by users in the SMSC who have access to the messaging system. Spying programs such as FlexiSpy7 enable intruders to automatically record all incoming and outgoing SMS

messages and then upload the logs to a remote server for later viewing and analysis.

2. Spamming

While e-markets are using SMS as a legitimate marketing channel, many people have had the in-convenience of receiving SMS spam. The availability of bulk SMS broadcasting utilities makes it easy for virtually everyone to send out mass SMS messages.

3. Flooding/Denial of Service (DoS) Attacks

Flooding or DoS attacks are made possible by sending repeated messages to a target mobile phone, making the victim's mobile phone inaccessible. Studies also show that weaknesses in the SMS protocol could be exploited to launch a DoS attack on a cellular phone network. For example, it was found that sending 165 text messages a second was enough to disrupt all the cell phones in Manhattan8.

4. SMS Phone Crashes

Some vulnerable mobile phones may crash if they receive a particular type of malformed short message. Once a malformed message is received, the infected phone becomes inoperable. Media reports have shown that mobile phones are vulnerable to this type of attack9.

5. SMS Viruses

There have been no reports of viruses being attached to short messages, but as mobile phones are getting more powerful and programmable; the potential of viruses being spread through SMS is becoming greater. In addition, the ability of SIM application toolkits that allows applications to access the dialing functions and phone book entries might make SMS suitable platform for spreading self-replicating virus.

6. Smashing (SMS Phishing)

SMiShing10 is a combination of SMS and phishing. Similar to an Internet phishing attack using email, attackers are attempting to fool mobile phone users with bogus text messages11.tricked into download a malware application into their mobile phones.

D. Sms Security Considerations

1. Message Transmission

When sending SMS messages via a web browser, security protection should be in place to prevent message disclosure, such as using Secure Socket Layer (SSL) to secure the transmission. For those applications that require secure transmission of a message, such as mobile banking, end-to-end encryption is advisable between the sender and the recipient. These transactional systems should have the end-to-end security built-in. For person-to-person communications, products such as CryptoSMS12 are available to help users encrypt SMS communications using strong encryption algorithms. This can help protect against possible SMS interception threats.

2. Storage Protection

In the case of large-scale SMS broadcasts, customer mobile phone contact lists should be kept confidential and properly protected should be implemented in accordance with privacy laws and regulations

3. User authentication

User login IDs and passwords should be used to authenticate users on web-based SMS services when sending short messages. User login IDs and passwords should not be disclosed to others. For secure transactions, user authentication should be protected by SSL.

4. Protection of PCs for sending messages

When sending short messages to an SMS gateway via the Internet, it is not advisable to use a public Internet terminal. If desktop utilities are used to send out SMS messages, the PC used to send the message should not be left unattended.

V. SHORT MESSAGE SERVICE (SMS)

SMS stands for short message service. Simply put, it is a method of communication that sends text between cell phones, or from a PC or handheld to a cell phone. The "short" part refers to the maximum size of the text messages: 160 characters(letters, numbers or symbols in the Latin alphabet). For other alphabets, such as Chinese, the maximum SMS size is 70 characters.

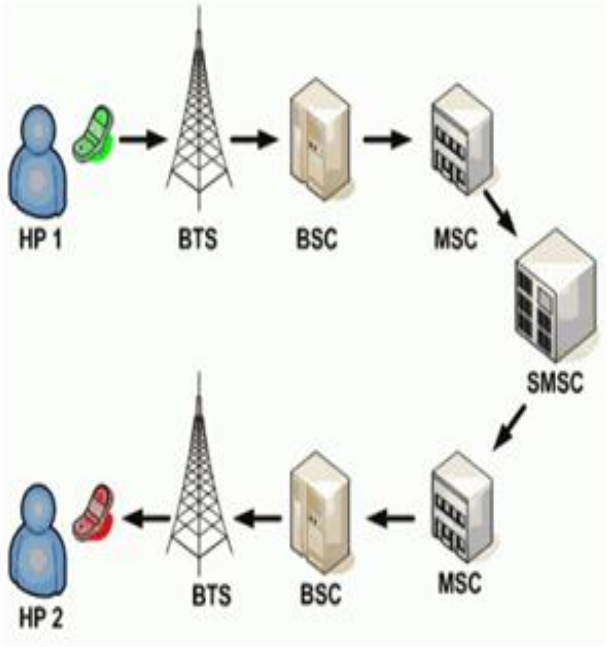

Figure 5: Working of SMS

A. Working of SMS

It is well-known that SMS service is a cell phone feature but indeed, SMS can also work on other computing devices such as PC, Laptop, or Tablet PC as long as they can accept SIM Card. SIM Card is needed because SMS service needs SMS center client which is built-in on the SIM Card. Figure 5 shows the how an SMS is working on multiple factors.

1. BTS

A base transceiver station(BTS) is a piece of equipment that facilitates wireless communication between user equipment(UE) and a network. UEs are

devices like mobile phones (handsets), WLL phones, computers with wireless internet connectivity, WiFi and WiMAX devices and others.

2. MSC

The mobile switching center (MSC) is the primary service delivery node for GSM/CDMA, responsible for routing voice calls and SMS as well as other services (such as conference calls, FAX and circuit switched data).[2] The MSC sets up and releases the end-to-end connection, handles mobility and hand-over requirements during the call and takes care of charging and real time pre-paid account monitoring.

3. SMSC

When SMS is transmitted from a cell phone, the message will be received by mobile carrier's SMS Center (SMSC), do destination finding, and then send it to destination devices (cell phone). SMSC is SMS service center which is installed on mobile carrier core networks. Beside as SMS forwarding, SMSC also acts as temporary storage for SMS messages. So, if the destination cell phone is not active, SMS will store the message and then deliver it after the destination cell phone is active. As additional, SMSC also notify the sender whether the SMS delivering is success or not. However SMSC cannot store the SMS message forever since the storage capacity is not unlimited. During the SMS delivering, sender cell phone and SMSC is actively communicating. So, if the non-active destination cell phones become active, SMSC directly notifies the sender cell phone and tell that the SMS delivering is success. This is how the SMS works in general. The following part describes the AES algorithm.

VI. ADVANCE ENCRYPTION STANDARDS ALGORITHM/ RIJNDAEL ALGORITHM

The Advanced Encryption Standard comprises three block ciphers, AES-128, AES-192 and AES-256. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. The block-size has a maximum of 256 bits, but the key-size has no theoretical maximum. The cipher uses number of encryption rounds which converts plain text to cipher text. The output of each round is the input to the next round. The output of the final round is the encrypted plain text known as cipher text. The input given by the user is entered in a matrix known as State Matrix [2] as shown in figure 6. Following are the four steps.

1. SubBytes Step: This step is same as SubBytes step of AES algorithm. In the S-Box Substitution step, each byte in the matrix is reorganized using an 8-bit substitution box. This substitution box is called the Rijndael S-box. This operation provides the non-linearity in the cipher. The S-box used is derived from the multiplicative inverse over GF (28), known to have good non-linearity properties. To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation. The S-box is also chosen to avoid any fixed points (and so is a derangement), and also any opposite fixed points. [7] This step causes confusion of data in the matrix. S-Box Substitution is carried out separately for LPT and RPT. This is the first step of iterative round transformation. The output of this round is given to the next round [3].

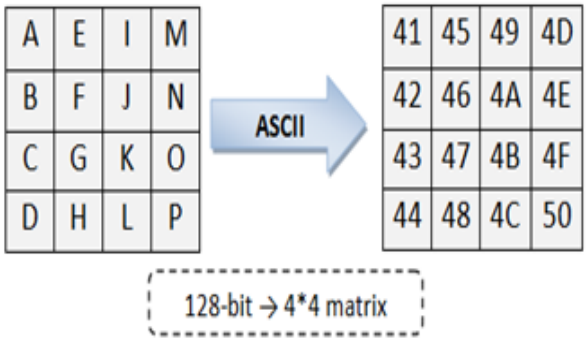

Figure 6: State matrix.

2. ShiftRows Step: The ShiftRows step is performed on the rows of the state matrix. It cyclically shifts the bytes in each row by a certain offset. The first row remains unchanged. Each byte of the second row is shifted one position to the left. Similarly, the third and fourth rows are shifted by two positions and three positions respectively. The shifting pattern for block of size 128 bits and 192 bits is the same[3].

3. MixColumns Step: In the MixColumns step, the four bytes of each column of the state matrix are combined using an invertible linear transformation [5]. A randomly generated polynomial is arranged in a 4*4 matrix. The same polynomial is used during decryption. Each column of the state matrix is XOR-ed with the corresponding column of the polynomial matrix. The result is updated in the same column. The output matrix is the input to AddRoundKey[3].

4. AddRoundKey: A round key is generated by performing various operations on the cipher key. This round key is XOR-ed with each byte of the state matrix. For every round a new round key is generated using Rijndael‟s key scheduling algorithm [3].

A. Decryption of the Proposed Algorithm

The encryption algorithm is referred to as the cipher and the decryption algorithm as the inverse cipher. In addition, the cipher and the inverse cipher operations must be executed in such a way that they cancel each other. The rounds keys must also be used in reverse order. [4] The Cipher Text which is formed of 256-bit 4*8 Matrix is the input for the decryption process [3].

B. Implementation

The algorithm can be implemented in any language. This algorithm can also be used in Image Processing. We have implemented it in java, java being an open source and platform independent language. The pseudo codes for the components of the cipher are given below [3].

1. Add Round key

```
public byte[ ][ ] addRoundKey(byte[ ][ ] state, byte[ ][ ]
                                                    roundkey)
{
    for (int i=0;i<4;i++)
    {
     for (int j=0;j<4;j++)
     {
state [i][j]=doExclusiveOR(state[i][j], roundkey[i][j]);
     }
   }
return state;
}
```

2. Substitute Bytes

```
public byte[ ][ ] subBytes(byte[][] state)
{
     for (int i=0;i<4;i++)
    {
       for (int j=0;j<4;j++)
       {
       int row = getFirstFourBits(state[i][j]);
       int column = getSecondFourBit(state[i][j]);
       state[i][j] = sBoxSubstitution(row,column);
       }
    }
 return state;
}
```

3. MixColumns

```
public byte[ ][ ] mixColumns(byte[ ][ ] state)
 {
      for (int c=0;c<4;c++)
       {
      state [c]=matrixMultiplication(state[c], polynomial);
        }
      return state;
}
```

C. Strength of the Algorithm

The cipher key used in the algorithm is of 128 bits. Therefore, to break the cipher key an attacker has to check 2128 possibilities which are practically almost impossible. Therefore, the Brute-force Attack fails on this algorithm. The flow of the algorithm makes sure that there is no fixed pattern in any of the steps of the algorithm. The components of the proposed algorithm have brought about strong diffusion and confusion. Therefore, statistical and pattern analysis of the ciphertext fails [4]. The most important security advantage is that no differential or linear attacks can break this algorithm [9].

VII. SMS APPLICATION

The application works in following way:

1. The user opens the application and authenticates using pattern lock.
2. User can either type new message or reply to an existing message.
3. If new message is selected, user enters the message and presses encrypt button after inserting the recipient's name. The user has to enter a cipher key before the message is sent. The cipher key is auto-generated if the user does not enter one.
4. If the user selects to reply to an existing message, he first decrypts the message by long pressing the message and then types in the reply. The user is asked to enter cipher key before the message is sent.
5. Once the cipher key is entered, the message is successfully sent and is shown in encrypted form in the thread.

A. Application Snapshots

Some of the snapshots of the application are shown below. It should be noted that due to obvious reasons we are not sharing the entire layout of the application. However, few of the important snapshots are given below.

1. Pattern Lock

As shown in figure 7 this is used by the user to authenticate his identity. The user may change the lock code once he authenticates and logs into the application. After 5 incorrect attempts the application closes.

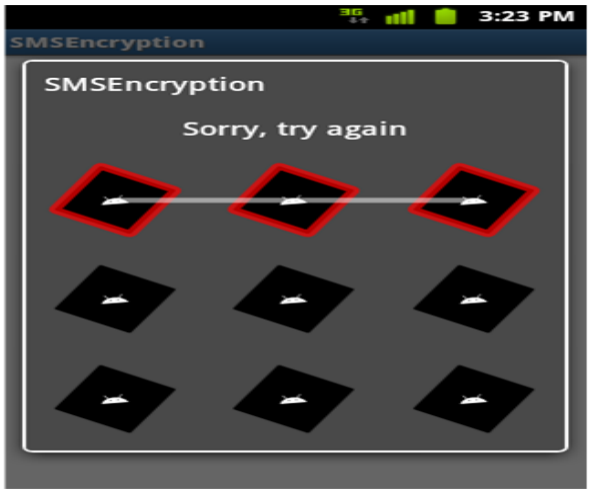

Figure 7: Pattern Lock

2. Create Message

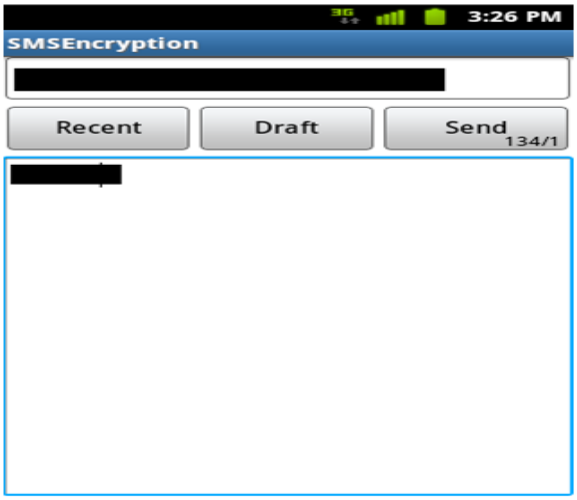

Figure 8: Create Message

The user types in the message along with the name of the sender. The relevant contact information is displayed in the dropdown menu as the user starts to write the name. He can then select the name and the number which is displayed in dropdown menu. If suppose user types „ro‟ in the name field then all the contacts having initials „ro‟ or containing „ro‟ as a sub-text are displayed in the dropdown menu below it along with the telephone number. As shown in figure 8 user may save the message as draft or send it by entering the cipher key. User can choose any recent contact from his call log by pressing „Recent‟ button.

3. Thread View

The messages in the application inbox are shown in form of thread. Long pressing on the thread gives option to delete the thread or open the contact information of the thread or call the contact to which the thread belongs.

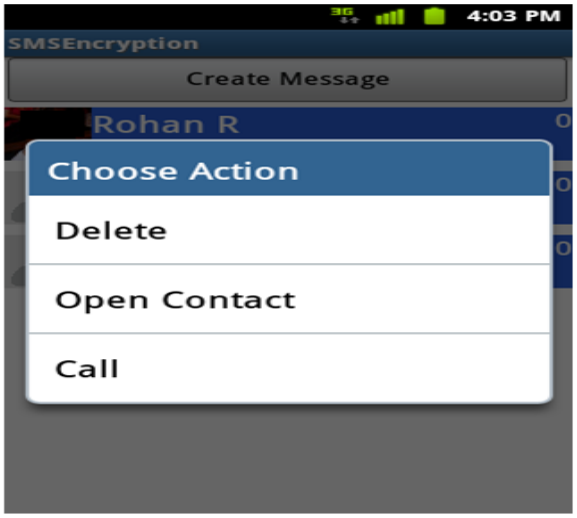

Figure 9: Message Inbox

B. Features of this Application

Following are some of the features of the application:

1. All messages in thread are displayed in encrypted format to both sender and receiver.
2. Long pressing the thread will pop-up an action box wherein the user can delete, view contact details or call the recipient.
3. Long pressing any message in the thread will pop-up an action box wherein the user can delete, forward or decrypt the message.
4. The cipher key is randomly generated if the user does not enter it.
5. Various settings such as notification settings, Display settings, Encryption settings, Tone settings, Personalization settings are available for the user‟s convenience.
6. This application is developed on Android platform. The reason behind using Android platform is similar to other operating systems for mobile devices; Android OS supports connectivity, messaging, language support, media support, Bluetooth etc. The main feature of android would be open source.

C. Goals of this application

The main goals of our application are:

1. Developing a secure SMS application.
2. Maintaining encrypted information of message recipients.
3. Decrypting of message as per users requirement.
4. Protection against misuse of message information.
5. High confidentiality and improved security.

1. Commercial Domain

In some commercial setups it is very must that information flow between various departments remain private and other department people should not come to know. This application can be used in such cases where the numbers and digits have more importance than documentations. The proposed application can be used for secured transactions on network [5].

2. Non-Commercial and Personal Use

There are sometimes when the user would like to keep talks between two people private and confidential. During such times, SMS encryption is a boon. An intruder would not be able to understand the message unless he has a proper authentication key.

D. Scope

The application is built on Android platform. Therefore, it can be used on any device which runs on Android operating system. This application can be used in industries for secured data transfer. Apart from commercial and business use, this application can be used for non-commercial and personal use. [6] The purpose of this application is secured data transfer between two devices.

E. Pseudo Codes of Android Application

We have written the code in Android language. The original codes are not given for obvious reasons. However, the main logic of the codes is given.

VIII. REFERENCES

[1] SMS document, Nokia, (2009, June). Available: http://wiki.forum.nokia.com/index.php/SMS.

[2] J. Li-Chang Lo, J. Bishop and J. Eloff. "SMSSec: an end-to-end protocol for secure SMS", Computers & Security, 27(5-6):154-167, 2007.

[3] P. Traynor, W. Enck, P. McDaniel and T. La Porta. "Mitigating Attacks on Open Functionality in SMS-Capable Cellular Networks", IEEE/ACM Transactions on In Networking, 17(1):40-53, 2009.

[4] GSM document, Short Message Service, (2009, July). Available: http://www.gsmfavorites.com/documents/sms/.

[5] SMS peer-to-peer protocol, Wikipedia, (2009, May).

[6] J.Daemen and V.Rijmen, AES Proposal: Rijndael, NIST‟s AES home page, http://www:nist:gov/aes. “Announcing the Advanced Encryption Standard (AES)”,

Federal Information Processing Standards Publication 197, November 2001.

[7] Priyanka Pimpale, Rohan Rayarikar and Sanket Upadhyay, "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.10, October 2011.

[8] Hassinen M.: SafeSMS 1.0 user manual. October 2004, Department of Computer Science, University of Kuopio.

[9] http://www.cs.uku.fi/~mhassine/SafeSMS/Manual en. pdf.

[10] G. Racherla, D. Saha, "Security and Privacy Issues in Wireless and Mobile Computing", Proceedings of 2000 IEEE International Conference on Personal Wireless Communications, Dec 17-20, 2000, pp.509-513.

[11] H. Marko, H. Konstantin, "Strong Mobile Authentication",Proceedings of 2nd International Symposium on WirelessCommunication Systems, Sept 5-7 2005, pp.96-100.

[12] Xinmiao Zhang and Keshab K. Parhi, "Implementation Approaches for the Advanced Encryption Standard Algorithm", 1531-636X/12, IEEE 2002.

[13] Chun Yan, Yanxia Guo, "A Research and Improvement Based on Rijndael Algorithm", 2009 First International Conference on Information Science and Engineering, Nanjing, Jiangsu China, December 26-December 28, ISBN:978-0-7695-3887-7.

[14] Advanced Encryption Standard, http://en.wikipedia. org/wiki/Advanced_Encryption_Standard.